



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/918,602	07/30/2001	Christopher P. Jalbert	04860P2441	5216

7590 11/20/2006
James C. Sheller
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER

PYZOCHA, MICHAEL J

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 11/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/918,602

Applicant(s)

JALBERT ET AL.

Examiner

Michael Pyzocha

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 October 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-41 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-41 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-41 are pending.
2. Amendment filed 10/10/2006 has been received and considered.

Claim Rejections - 35 USC § 112

3. The filed amendment overcomes the rejections under the second paragraph of 35 USC 112.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-5, 12-13, 17-22, 24, 26, and 34-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang, U.S. Patent No. 5,953,424, in view of Menezes (Menezes, Alfred J. Handbook of Applied Cryptography. CRC Press. 1997. pages 234-237).

Art Unit: 2137

As per claims 1, 20, 21, 22, 24, and 38-40, the applicant describes a cryptographic method with the following limitations which are met by Vogelesang in view of Menezes:

a) generating, at a first entity, a first public key M_B , the first public key M_B being session specific (Vogelesang: Col 16, lines 33-35);

b) receiving, at a first entity, a second public key M_A , the second public key M_A being session specific (Vogelesang: Col 16, lines 36-38);

c) generating, at the first entity, a first session key K_B and a first secret S_B . the first session key K_B being different from the first secret S_B , both the first session key K_B and the first secret S_B being computed from the second public key M_A (Vogelesang: Col 16, lines 39-67);

d) encrypting, at the first entity, a first random nonce N_B with the first session key K_B or the first secret S_B to obtain a first encrypted result (Vogelesang: Col 16, lines 43-67);

e) encrypting, at the first entity, the first encrypted result with the other one of the first session key K_B or the first secret S_B to obtain an encrypted random nonce (Vogelesang: Col 16, lines 43-67; Menezes: pages 234-237);

f) transmitting the encrypted random nonce from the first entity to the second entity (Vogelesang: Col 16, lines 64-67);

g) receiving a response to the encrypted random nonce
(Vogeleang: Col 17, lines 19-24);

h) authenticating through determining whether the response includes a correct modification of the first random nonce N_B .
(Vogeleang: Col 17, lines 28-30).

Vogeleang teaches a cryptographic method which meets limitations of the above claim (except for part e). Specifically with regards to part e), Vogeleang teaches that a first random nonce may be encrypted at the first entity with a session key to obtain a first encrypted result (e.g. Col 16, lines 64-67) (part d). Vogeleang also teaches a number of secrets that are generated using the second public key (e.g. T , Y_D , and other values which qualify as a "secret" under MPEP 2111). However, Vogeleang does not appear to suggest that the first encrypted result may be double encrypted.

Menezes teaches that encipherment of a message more than once "may increase security" (Menezes: page 234). Further, illustrates the process whereby a message may be encrypted once with a first key and a second time with another key (Menezes: page 234, part (a)). Combining the ideas of Menezes with Vogeleang facilitates a system in which a message may be encrypted once with a first key (e.g. session key) (part d) and a second time with another key (e.g. secret). It would have

Art Unit: 2137

been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Menezes with those of Vogelesang because doing so may increase security.

As per claim 2, the applicant describes the method of claim 1, which is met by Vogelesang in view of Menezes, with the following limitations which are also met by Vogelesang:

a) generating the first secret S_B from at least a first password P_B and the first public key M_B (Vogelesang: Col 16, lines 39-67).

As per claims 3 and 4, the applicant describes the method of claim 1, which is met by Vogelesang in view of Menezes, with the following limitation which is also met by Vogelesang:

Checking whether a received modification of the first random nonce N_B equals a modification of the first random nonce N_B applied by the first entity (Vogelesang: Col 17, lines 25-37).

As per claim 5, the applicant describes the method of claim 1, which is met by Vogelesang in view of Menezes, with the following limitation which is also met by Vogelesang:

a) generating a first random number R_B (Vogelesang: Col 16, lines 39-40);

b) computing the first session key K_B from the second public key M_A raised to the exponential power of the first random number R_B , modulo a parameter B_B (Vogelesang: Col 16, lines 39-42).

As per claims 12 and 13, the applicant describes the method of claim 1, which is met by Vogelesang in view of Menezes, with the following limitation which is also met by Vogelesang:

Wherein the first random nonce is encrypted using a symmetrical encryption algorithm (Vogelesang: Col 16, lines 64-67).

As per claims 17-19, the applicant describes the method of claim 1, which is met by Vogelesang in view of Menezes, with the following limitation which is also met by Vogelesang:

a) extracting the second random nonce N_A from the response (Vogelesang: Col 16, line 39 to Col 17, line 28);

b) modifying the second random nonce N_A to obtain a modified second random nonce (Vogelesang: Col 16, line 39 to Col 17, line 28);

c) encrypting the modified second random nonce using the first session key K_B and the first secret S_B to obtain an encrypted package (Vogelesang: Col 16, line 39 to Col 17, line 28);

d) transmitting the encrypted package from the first entity (Vogelesang: Col 16, line 39 to Col 17, line 28).

As per claim 26, the applicant describes the method of claim 24, which is met by Vogelesang in view of Menezes, with the following limitations which are met by Vogelesang:

- a) generating a first random number R_B (Vogelesang: Col 16, lines 39-40);
- b) computing the first session key K_B from the second public key M_A raised to the exponential power of the first random number R_B , modulo a parameter B_B (Vogelesang: Col 16, lines 39-42).

As per claims 34-37, the applicant describes the method of claim 24, which is met by Vogelesang in view of Menezes, with the following limitation which is also met by Vogelesang:

- a) generating a first random number N_B (Vogelesang: Col 16, line 33 to Col 17, line 27);
- b) encrypting a combination of the first random number N_B and the modified second random number (Vogelesang: Col 16, line 33 to Col 27, line 27).

5. Claims 6-9, 11, and 27-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang in view of Menezes

Art Unit: 2137

in further view of Wu (Wu, Thomas. "The Secure Remote Password Protocol". November 11, 1997. Stanford University. pages 1-17).

As per claims 6-9, 11, 27-30, and 32, the applicant describes the method of claims 1 and 27, which are met by Vogelesang in view of Menezes, with the following limitation which is also met by Wu:

Wherein the first secret S_B is generated using a combining function f_B on at least a first password P_B and the first public key M_B (Wu: page 7).

Vogelesang in view of Menezes teaches all the limitations of claim 1. However, Vogelesang in view of Menezes do not appear to teach that a secret may be generated from a combining function of a password and a public key. Wu teaches that a secret may be generated from a combining function of a password and a public key. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Wu with those of Vogelesang in view of Menezes and utilize a combining function to create a secret because doing so facilitates a secure generation of the secret.

As per claims 10 and 31, the applicant describes the method of claims 9 and 30, which are met by Vogelesang in view of Menezes in further view of Wu, with the following limitation:

Wherein the one-way hash function is one of the Secure Hash Algorithm, the Message Digest 5, Snefru, Nippon Telephone and Telegraph Hash, and the Gosudarstvenny Standard.

Vogelesang in view of Menezes in further view of Wu teach all the limitations of claim 9. However, the combination appears to be silent as to what type of one-way hash function is employed. Examiner takes official notice that at least the Secure Hash Algorithm is common and known in the art. It would have been obvious to one of ordinary skill in the art to utilize the Secure Hash Algorithm because it is a common method of securely creating a hash.

As per claims 14-16,25, and 33, the applicant describes the method of claim 1 and 24, which are met by Vogelesang in view of Menezes, with the following limitation which is met by Menezes:

a) wherein encrypting the first random nonce N_B includes superencrypting the first random nonce N_B (Menezes: pages 234-237);

Art Unit: 2137

As per claim 41, the applicant describes the method of claim 40, which is met by Vogelesang in view of Menezes, with the following limitation which is also met by Vogelesang:

Wherein the network is a network operating according to a hypertext transfer protocol and the first public key M_B is transmitted for session key exchange before the encrypted second random number is received (Vogelesang: Col 1, lines 12-14; Col 16, lines 25-67).

Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang in view of Menezes.

As per claim 23, the applicant describes the system of claim 22, which is met by Vogelesang in view of Menezes, with the following limitation:

A network operating according to a hypertext transfer protocol and the first public key M_B is transmitted with the encrypted random nonce for session key exchange;

Vogelesang in view of Menezes does not disclose transmitting the first public key M_B with the encrypted random nonce. Applicant's failure to argue the previous official notice of the subject matter of claim 23 is taken as acquiescence that the subject matter of claim 23 is obvious (See

Art Unit: 2137

MPEP 2144.03). It would have been obvious to one of ordinary skill in the art at the time the invention was filed to transmit a key with a nonce because doing so is more efficient than having to make two separation transmissions for the key and the nonce.

Response to Arguments

6. Applicant's arguments filed 10/10/2006 have been fully considered but they are not persuasive. Applicant argues that Vogelesang in view of Menezes does not teach both the first session key and first secret being computed from the second public key and Wu fails to teach a combining function to generate a secret.

With respect to Applicant's argument that Vogelesang in view of Menezes does not teach both the first session key and first secret being computed from the second public key because Menezes teaches that the two encryption keys are independent of each other and therefore cannot be computed from the same public key, Menezes does teach this fact in definition 7.29, but in definition 7.30 Menezes teaches that the keys need not be independent. Therefore the combination of Vogelesang and Menezes teaches both the first session key and first secret

Art Unit: 2137

being computed from the second public key as put forth in the above rejection.

With respect to Applicant's argument that Wu fails to teach a combining function to generate a secret the combination of Vogelesang and Menezes teaches the generation of a secret, and Wu is relied upon for the teaching of a combining function used in a mutually authenticated key exchange algorithm. Furthermore, the combining function is used to generate B which is used to generate S and S is the secret so the combining function is used to generate a secret.

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 2137

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER